NDIA 14th Annual Security Technology Symposium
"New Dimensions in Security Threats & Countermeasures"
June 17, 1998

Introduction

I am very pleased to be here today and to have this opportunity to tell you about some steps the FBI is taking to address critical infrastructure protection. I also commend the National Defense Industrial Association for holding this symposium, which brings together representatives from government and the private sector and contributes to our dialogue on this extremely important subject.

Three-sentence summary

There are three points that I would like to elaborate on today:

First, the domestic infrastructure is at risk as never before. Today's environment presents new threats, new vulnerabilities, and new challenges that must be confronted. Failure to address them can have enormous adverse effects, both for industry and for the economy.

Second, government and industry are finding new ways to jointly address infrastructure threats and vulnerabilities. Unlike in the past, when national security was largely a government responsibility, today the responsibility has to be a shared one, with the private sector taking on an increasingly important role.

Third, the National Infrastructure Protection Center is a new FBI organization for protecting the domestic infrastructure. At the FBI we believe that the way to address infrastructure protection is through partnerships with the private sector. We need a two-way street for the flow of information between government and the private sector. The NIPC is designed to do just that.

The Networked infrastructure

Not so long ago, there was little risk of a large-scale infrastructure disruption. Until recently, only a rare and isolated occurrence, such as an earthquake or tornado or an accidental power outage could knock out a critical service over a broad area. The physical breadth of the infrastructures made it difficult for any person or thing to cause more than an isolated and transient disturbance. And physical security measures adopted to prevent theft or vandalism generally also kept out those who might try to do more serious damage. We were able to build strong fences and be fairly sure that we were protected not only against thieves and vandals, but also terrorists and anarchists. And we took comfort in knowing that the large size of our country and its geographic separation from other countries made it difficult for foreign adversaries to launch a widespread attack on our infrastructure.

Today things are dramatically different. For while information technology can increase efficiency and productivity, and can give a nation a competitive advantage, dependence on information systems can create new vulnerabilities. Leadership in information technology is one of the things that give the United States a competitive advantage in the global economy. But it also opens us up to new types of harm that can undermine the national economy and our national security.

The infrastructure is at risk

I don't think I have to convince this audience of the need to protect the electronic networks of the domestic infrastructure.

In the past few years our society has moved on-line. Computers have found more application in our lives than one can list. Millions of cyber-citizens use Local Area Networks, the Internet, and the banking networks. No longer only for the technological elite, network technology is now accessible to the masses. We are truly a networked society.

In addition, telecommunications is now a truly global enterprise. Satellite communications, the Internet, and foreign ownership of telecommunications carriers in the U.S. have all combined to undermine the idea of a "national" information infrastructure. This means that geographic separation no longer helps fend off foreign adversaries. Now a laptop computer and a telephone connection can make it as easy to break into an infrastructure's control network from St. Petersburg, Russia, as from St. Petersburg, Florida.

Other dynamics are at work in the marketplace. There is a move towards open system architectures and commercial off-the-shelf technology. High-tech companies are rushing new products to market without a complete understanding of their security vulnerabilities. And in the many sectors, software development is concentrated in a few specialized companies. As a result, there is an increased chance that a fault can have a widespread impact.

At the same time, changes in the business environment are occurring in all sectors of the infrastructure. Deregulation, downsizing, increasing competition with new entrants into infrastructure markets, and

outsourcing of core functions are some of the factors that together are putting new stress on security processes and can cause new vulnerabilities.

A third reason that the infrastructure is at risk is the increasingly sophisticated threat.

In the physical world, the range of people or groups that would have the means and motive to cause widespread destruction of an infrastructure is relatively limited – terrorist groups and hostile nations are the most likely actors. But the accessibility of the information infrastructure, global connectivity, and the rapid growth of a computer-literate population combine with the result that the means to conduct a cyber attack can be in the hands of a frighteningly large number of people.

Perhaps the greatest threat today comes from insiders. Insiders have the advantage of not needing to break into computer systems from the outside, but only to use – or abuse – their legitimate access. These individuals often have intimate knowledge of where the most sensitive information is stored, how to access the information, and how to steal or damage the data. They can make attractive exploitation targets for hostile agents. The greatest insider risk may not be your own employees. It could be the insiders or your hardware of software vendor, or insiders associated with other infrastructures like telecommunications who could target your sector.

Recreational hackers are also increasingly dangerous, in part because of the widespread availability of "cracking" tools on hacker websites. One no longer needs to have an advanced understanding of computers and the Internet to successfully crack into a company's systems. Rather, one needs only to download sophisticated hacking tools from the Internet, then "point and click" to launch an attack on any number of target sites. The results of these cyberspace joyrides could be widespread and severe, regardless of the intent.

Consider this real-world incident:

In March of last year, a teenager hacked into the local telephone company in Worcester, Massachusetts, shutting down phone service to the area's airport control tower and approximately 600 customers for over six hours. He broke into the telephone system using a common personal computer equipped with a modem. The main control tower at the airport was unable to communicate with the airport fire department or other services. The airport's main radio transmitter and a circuit which enables aircraft to send an electrical signal to activate the runway lights on approach were not operational. According to prosecutors, the juvenile was unaware of the seriousness of his actions.

If a teenager can do this for kicks, imagine what a coordinated, focused attack on infrastructure information networks could do. To date, the United States has not experienced this sort of attack, but it is not hard to extrapolate from intrusions we have seen. This is a possibility we must try to prevent from ever becoming reality.

In addition, we expect foreign intelligence services and hostile nations to increasingly use cyber tools to conduct espionage or engage in "information warfare" against us. Because no nation or group hostile to the United States can match us in traditional military firepower, none would be likely to take us on in a frontal attack. Rather, they would hit us where we are most vulnerable. And one of those vulnerabilities is our reliance on information technologies for command and control of our national security activities as well as for the daily functioning of our privately owned critical infrastructures.

Vision for the Future

What, then, is to be done? How can we protect our critical infrastructures in such a dynamic environment? The answer, I believe, lies in dialogue – dialogue between industry and the government, as well as dialogue with our international partners, to jointly identify and address the real threats and actual vulnerabilities. Some mechanisms already exist between the government and industry for jointly dealing with computer security incidents:

The Suspicious Activity Reporting System is one example. Suspicious Activity Reports are used by financial institutions to report potentially fraudulent activity associated with electronic financial transactions. Reportable activities are defined by statute, which also specifies the measures to be taken to protect the information that is collected.

The ANSIR program is another. ANSIR stands for Awareness of National Security Issues and Response. This FBI program is designed to provide unclassified national security threat and warning information to U.S. corporations, law enforcement agencies, and other government organizations. Information is disseminated nationwide via e-mail and fax through the fifty-six FBI field offices. All told, ANSIR has the capacity to reach over 100,000 addressees.

These important programs, however, are somewhat limited in what they set out to do in the context of protecting the infrastructure. In practice, each provides for information flow that is primarily in one direction. Our vision is to build a two-way street for the flow of intelligence information and incident data between the government and industry. The government, with access to national intelligence and law enforcement information, can develop a threat picture that no one in the private sector could develop on their own. We'd like to share this with the industry. At the same time, we'd like to learn from the industry about the intrusion attempts and vulnerabilities they are experiencing. This will help us paint the threat picture more completely, and will give us a head start on preventing or disabling a nascent attack. I believe this two-way dialogue is the best way to deal with our common concern about security.

Two-way dialogue is also important with our international partners, which include foreign governments and law enforcement agencies. The benefits of such dialogue are clear, as demonstrated during a recent investigation known as Solar Sunrise, in which U.S. and Israeli authorities cooperated to identify and apprehend a group of hackers who were penetrating U.S. defense networks.

Of course, we would need to establish the parameters of the relationship. The information needs to be timely. We need clear limits on what is to be shared – limits that are both legal and equitable to both parties. And we need to make sure the information that is shared is protected. But now is the time to start building this relationship.

Impediments

If cooperation between government and industry is needed to squarely address a problem of such import, why don't we just get on with it? Well, actually it is not quite that easy. There are impediments to cooperation – sometimes real, sometimes perceived – on both sides. Let me describe a few as I understand them.

First of all, industry has historically addressed its own security challenges very effectively. It is hard to argue with decades of success. But the vulnerability and threat environment has changed dramatically in recent years. Networks have become too integrated for this independent approach. Your vulnerabilities are to a large extent my vulnerabilities, and vice versa. An infrastructure sector can't solve network security problems in isolation.

Fear of adverse publicity can also be an impediment. For a corporate leader to talk about infrastructure vulnerabilities is to invite questions of reliability and potential erosion of customer confidence. I understand the desire to keep this kind of information to yourself. But I can tell you that we at the FBI are committed to preserving the confidentiality of proprietary data during investigations and prosecutions to the full extent possible under the law. And keep in mind that a serious security incident could also have an adverse effect on customer confidence.

The competitive environment might also be seen as impediments to information exchange. If managing network risk involves dialogue and cooperation among competitors, both the natural forces of the marketplace can put a damper on cooperation. But there are ways of sharing without losing competitive advantage or running afoul of regulators. The Network Security Information Exchange forums established by the government and the telecommunications industry are probably the best example of the benefits of a controlled dialogue on infrastructure vulnerabilities. These forums bring together the major players of the telecom industry, the intelligence community, the FBI, and other government agencies to address network security. They have been operating successfully for years. Nondisclosure agreements, strict control over participation, and strong commitments to respect the confidentiality of data go a long way towards allowing competitors and the government to cooperate.

And there is the question of costs and benefits. "What's in it for me?" is a fair question for the industry to ask. I understand a reluctance to share incident and vulnerability information with the Federal Government if the cost of reporting outweighs the benefit received in return. But I can tell you that the FBI is committed to the idea of a two-way street for the flow of information between government and industry. We know we have to add value if we want a partnership to work.

From the government's perspective, protecting sources and methods is always a chief concern when disseminating intelligence information. By its nature, this information has to be handled carefully so as not to compromise the government's sources and collection methods. Access to classified material requires a government-issued security clearance and a legitimate need to know. With the right ground rules, though, we can make classified information available, and we are committed to doing so.

Also when dealing with a criminal investigation, law enforcement authorities must be concerned about rules of criminal procedure so as not to jeopardize the prosecution of the case. Specific rules prohibit sharing of certain information, such as grand jury information, and this can affect how information is handled. But we have learned that there are ways to sanitize the data while still providing a tremendous amount of useful information for the private sector.

The way ahead

None of these impediments needs to prevent dialogue. We believe this, and I'd like to tell you about two ways we are acting on this belief.

NIPC

In February of this year, the FBI created the National Infrastructure Protection Center, or NIPC. The NIPC's mission is to detect, deter, prevent, assess, warn, respond to, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures. Notice the emphasis on prevention. Our job is not simply to investigate and respond to attacks after they occur, but to learn about them beforehand and prevent them. This requires collecting and analyzing information from all available sources, and disseminating analyses and warnings of possible attacks to potential victims, whether in the government or private sector.

This broader mission is something that the FBI cannot do alone. It requires the combined efforts of many different government agencies. The Departments of Defense, Treasury, Energy, and Transportation and others have significant roles.

We also need the involvement of State governments because they own, operate, or have jurisdiction over some of the critical infrastructures and because their agencies are often the first responders in the event of a crisis.

And, perhaps most importantly, this mission requires the intensive involvement of the private sector. Private industry owns and operates most of the infrastructures and has the greatest expertise understanding of the technical problems and solutions. Industry also has the only direct knowledge of the real-world intrusions they are experiencing. Individual security incidents at network control centers across the industry could be part of a larger coordinated attack. Who can put the pieces together if no one says anything? We simply must ask the private sector to be involved with infrastructure defense.

Recognizing the roles of all these players, the NIPC is designed on the notion of a partnership. Partnership begins with inclusive representation, and the NIPC is being staffed with representatives from the other critical federal agencies, from State and local law enforcement, and from private industry, in addition to the FBI. This will foster the sharing of information and expertise, and improve coordination in the event of a crisis. And we will augment the physical presence of these representatives by establishing electronic connectivity to the many different entities in government and industry who might have, or need, information about threats to our infrastructures.

When fully staffed, the FBI will have 23 Special Agents at the NIPC, complemented by 76 Special Agents serving on Computer Investigation and Infrastructure Threat Assessment teams in each of the FBI's Field Offices. The NIPC will also have personnel from other government agencies and the private sector, for a total in-house staff numbering 125. This team will carry out the NIPC mission of analysis, warning, investigation, outreach, and coordination.

We have a lot of work to do in order to build the trusted relationships we need with your industry and the other infrastructure sectors. This will take time. But we are committed to this process, and we are looking forward to working with the private sector in a true win-win partnership.

InfraGard

A second example of our commitment to two-way partnership is InfraGard, a pilot project sponsored by the FBI's Cleveland Field Office. The name "InfraGard" refers to "guarding the information infrastructure." The program is a cooperative effort in the exchange of information between the business community, academic institutions, the FBI, and other government agencies to protect the information infrastructure.

InfraGard features an alert network that members can use to report intrusions. Reports are sent to the FBI via encrypted e-mail in two forms: a detailed description and a sanitized description. The FBI uses the detailed description to analyze the incident, identify trends, and open an investigation if warranted.

However, only the sanitized version is shared with other InfraGard members. The beauty of this procedure is that the reporting organization can choose the words to describe the intrusion to their competitors. InfraGard also features a secure website that members can use to obtain information about recent intrusions and infrastructure protection efforts, access original research on security issues, and confer with other members. The program also offers seminars and training to educate members on how they can prevent and respond to infrastructure attacks.

InfraGard membership is large and diverse. Currently the Cleveland InfraGard has approximately fifty-six member organizations, including KeyCorp, the Federal Reserve, TRW, Ameritech, Case Western Reserve University, and many government agencies such as FAA, NASA, and city and county agencies. Potential members must sign a membership agreement and a confidentiality pledge. And they must make a commitment to actively participate.

InfraGard is an experiment. We have high hopes that InfraGard will prove successful, and if it does we plan to move to a national system on the same model which would be managed by the NIPC.

Conclusion

In conclusion, I'd like to stress that the electronic infrastructure of the United States is at risk today as never before. This infrastructure is a critical national resource.

It is at risk because of new vulnerabilities, changes in the business environment, and the emergence of increasingly sophisticated threats.

I believe that the government and the private sector have security interests in common. But neither can address these security interests alone. The National Infrastructure Protection Center and InfraGard are two concrete steps we at the FBI are taking to build partnerships with the private sector to prevent and manage increasingly serious threats to critical United States infrastructures.

Let us get on with it. Let us – government and industry – join forces to defend against the Information Age threats that can disable our critical infrastructures. Let us not wait any longer.

Interested U.S. corporations should provide their email address, position, company name and address as well as telephone and fax numbers to the national ANSIR Email address at ansir@leo.gov. Individual ANSIR Coordinators in the respective field divisions will verify contact with each prospective recipient of ANSIR Email advisories.